

Santeri Kangaskolkka

SEAMLESS MPLS

Opinnäytetyö
Tietotekniikka

Joulukuu 2017



**Kaakkois-Suomen
ammattikorkeakoulu**

Tekijä/Tekijät	Tutkinto	Aika
Santeri Kangaskolkka	Insinööri (AMK)	Joulukuu 2017
Opinnäytetyön nimi Seamless MPLS		33 sivua
Toimeksiantaja KyAMK		
Ohjaaja Vesa Kankare		
Tiivistelmä <p>Opinnäytetyön tarkoituksena on tutustua Seamless MPLS-verkkoratkaisuun sekä kartoittaa ICT-laboratorion laitteiden mahdollisuuksia simuloida Seamless MPLS-verkkoja. Seamless MPLS-teknologia on yleisessä käytössä maailman suurimmissa operaattoriverkoissa ja on elintärkeä osa nykyaikaista verkkoinfrastruktuuria.</p> <p>Opinnäytetyön teoriaosuuden tarkoituksena on selvittää Seamless MPLS-teknologian perusteita sekä selittää sen toimintaa suurissa operaattoriverkoissa. Se käsittelee myös MPLS-tekniikan perusteita, sillä opinnäytetyön aiheen ymmärtämiseksi on tärkeä ymmärtää MPLS-protokollan perusteet.</p> <p>Teoriaosan hallinnan jälkeen työhön tehtiin kolme erilaista harjoituskonfiguraatiota, joista ensimmäisen oli tarkoitus tutustua tarkemmin Seamless MPLS-tekniikkaan vaadittaviin teknologioihin, kuten MPLS-protokollaan. Toisen ja kolmannen harjoituksen tarkoituksena oli selvittää ICT-Laboratorion laitteiden ja virtuaalialustan mahdollisuutta simuloida Seamless MPLS-verkkoa.</p> <p>Harjoitusten tuloksena todettiin ICT-Laboratorion virtuaalialustan olevan sopiva Seamless MPLS-teknologian simulointiin. Sen avulla on mahdollista suurempiakin Seamless MPLS-ratkaisuja, jotka auttavat huomattavasti operaattoriverkkojen ymmärtämistä laboratorioympäristössä.</p>		
Asiasanat MPLS, protokollat, suuralueverkot, ICT-laboratorio		

Author	Degree	Time
Santeri Kangaskolkka	Bachelor of Engineering	December 2017
Thesis title		33 pages
Seamless MPLS		
Commissioned by		
Kymenlaakso University of Applied Sciences		
Supervisor		
Vesa Kankare		
Abstract		
<p>The goal of this thesis was to study the technology and architecture used in Seamless MPLS solutions and map the possibilities to simulate such networks in ICT-Laboratory in Kymenlaakso University of Applied Sciences. Seamless MPLS is a vital part of largest operator networks and is widely used all around the world.</p> <p>The object of the thesis theory part is to make clear the basics of the Seamless MPLS technology and why it is used in large operator networks. It also covers the basics of MPLS-technology, because to understand the thesis subject it is essential to understand the basics of MPLS protocol.</p> <p>After the completion of theory part, three practice configurations were made. The subject of first configuration was to clarify the underlying techniques of Seamless MPLS, such as normal MPLS. The second and third practice configurations were made to map out the possibility of simulating Seamless MPLS network in ICT-laboratory.</p> <p>Results of the practice configurations showed that the virtual platform can simulate Seamless MPLS networks. It can be used to implement larger Seamless MPLS configurations to further understand the fundamentals of operator networks.</p>		
Keywords		
MPLS, protocols, metropolitan area networks, ICT-laboratory		

SISÄLLYS

KÄYTETYT LYHENTEET JA TERMIT	6
1 JOHDANTO	7
2 MPLS.....	8
2.1 Leimakytkentä.....	8
2.2 MPLS-operaatiot.....	9
2.3 LDP ja BGP-LDP	11
2.4 MPLS-TE	12
3 SEAMLESS MPLS.....	13
3.1 Verkon rakenne	14
3.1.1 Pääsyverkko, PE ja CE.....	14
3.1.2 Keräilyverkko	15
3.1.3 Area Border Router ja RR.....	15
3.1.4 Ydin.....	16
3.2 Leimareititys.....	17
3.3 Hierarkia	18
3.4 Skaalautuvuuden parantaminen	19
3.4.1 MPLS Downstream-On-Demand	20
3.4.2 Segment routing	20
4 VERKON VIKASIIETO.....	21
4.1 Palvelu- ja kuljetustason redundanttisuus.....	21
4.1.1 BGP-tunnelin redundanttisuus	21
4.1.2 LDP-Tunneleiden redundanttisuus	22
5 HARJOITUSTYÖ	23
5.1 Ensimmäinen harjoituskonfiguraatio	23
5.2 Toinen harjoituskonfiguraatio.....	24
5.3 Kolmas harjoitus	26
5.4 Client-Client I2VPN	27

6	PÄÄTELMÄT	30
	LÄHTEET	32
	LIITTEET	

KÄYTETYT LYHENTEET JA TERMIT

ABR	Area Border Router
BGP	Border Gateway Protocol
CE	Customer Edge
DOD	Downstream on Demand
FEC	Forward equivalence class
FRR	Fast Reroute
IGP	Interior Gateway Protocol
	Intermediate System-to-Intermediate Sys-
IS-IS	tem
LDP	Label Distribution Protocol
LSP	Label Switched Path
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
PE	Provider Edge
PHP	Penultimate hop popping
QOS	Quality of Service
RR	Route-Reflector
RSVP	Resource Reservation Protocol
TE	Traffic Engineering
VPN	Virtual private network

1 JOHDANTO

Internetin käyttäjäluku on kasvanut tasaisesti jo vuosia ja on arvioitu, että jopa lähes puolella maapallon väestöstä on jonkinlainen pääsy internettiin (Statista 2017b). Tämä luo suuria hankaluuksia internetin palveluntarjoajille käyttäjien kasvavan kysynnän, sekä verkon nopeuksien noustessa. Skaalautuvuus onkin siis tärkeää nykyaikaisissa verkoissa ja varsinkin internetin palveluntarjoajille tämä on elinehto. Siitä on tullut haastavampaa vuosien saatossa, kun verkot ovat kasvaneet yhä suuremmiksi varsinkin mobiililaitteiden kasvavan suosion vuoksi. Jo puolet nykyisistä selainhauista tulevat mobiililaitteiden kautta (Statista 2017a).

Seamless Multiprotocol Label Switching on yksi vaihtoehto tämän ongelman helpotukseen, sillä se parantaa Multiprotocol Label Switching (MPLS) -verkon skaalautuvuutta jakamalla sen osiin. Suurin osa jo olemassa olevista alueverkoista on MPLS-teknologian alaisia, joten Seamless MPLS on niiden luontainen jatkumo. Se mahdollistaa runkoverkon helpon suunnittelun ja skaalauksen, sekä siirtää MPLS-hallinnan yhteen isoon alueeseen monen pienen sijaan. Sen parhaita käyttökohteita ovatkin suuret yritysverkot, sekä internetin palveluntarjoajien runkoverkot.

Oleellisin aiempi opinnäytetyötä sivuuttava aihe on Riku Koivulan opinnäytetyö Core Hiding Migration, jossa käsitellään palveluntarjoajien tapaa piilottaa oma verkkonsa. Tämä opinnäytetyö kuitenkin keskittyy enemmän MPLS:n mahdollisuuksiin ja skaalautuvuuteen. Opinnäytetyössä sivutaan myös kappaleen verran Samu Varkaman Segment Routing- opinnäytetyötä ja sen mahdollisuutta toimia Seamless MPLS-teknologian apuna.

Opinnäytetyön tarkoituksena on tutustua Seamless MPLS-teknologiaan ja sen erilaisiin ominaisuuksiin ja mahdollisuuksiin. Lisäksi työssä tehdään kolme harjoituskonfiguraatiota, joiden tarkoituksena on varmistaa aiheen simulointimahdollisuus Kaakkoissuomen ammattikorkeakoulun ICT-Laboratorion virtuaalialustalla.

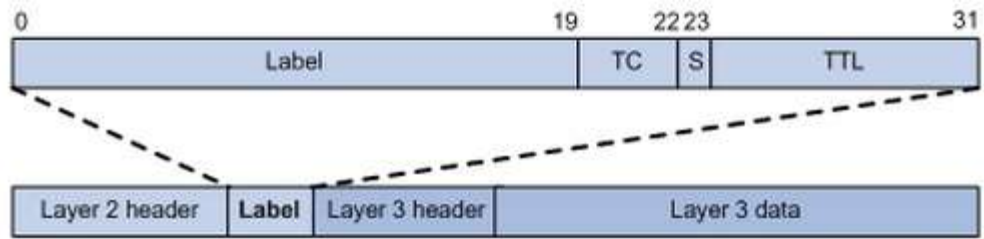
2 MPLS

Multiprotocol Label Switching eli MPLS on tekniikka, joka alkoi yleistyä 2000-luvun alussa. Sitä voidaan pitää OSI-mallin mukaisesti 2.5 tason tekniikkana, sillä se lainaa 2. ja 3. tason perusteita ja toimii myös molemmilla tasoilla. Internetin käytön yleistyessä rajusti verkot monimutkaistuivat ja tarvittiin tekniikka, joka yksinkertaistaisi verkkoja ja samalla nopeuttaisi näitä. MPLS suunniteltiin vanhempien tekniikoiden hyviä puolia ja heikkouksia silmällä pitäen. MPLS rupesi hitaasti syrjäyttämään vanhempia tekniikoita kuten ATM ja Frame Relay ja on nykyään yksi eniten käytetyimmistä tekniikoista maailmalla. Se myös tukee suurta joukkoa erilaisia verkkoprotokollia, joten se voidaan implementoida lähes minkälaiseen verkkoon tahansa.

MPLS tarvitsee toimiakseen reititysprotokollan, jotta se voi vaihtaa leimatietoja reitittimien välillä. Tästä syystä MPLS tarvitsee aina muita tekniikoita toimiakseen, joten häiriöt näissä alemmissa tekniikoissa voivat olla katastrofaalisia MPLS:n kykyyn ohjata paketteja. Tätä voidaankin pitää yhtenä MPLS-tekniikan suurimmista haitoista. Etuina sillä on normaaliin IP-pohjaiseen verkkoon esimerkiksi nopeampi paketin reititys ja QoS-hallinta. Suurena etuna on myös siihen lisättävät palvelut, joiden avulla voidaan liikennöidä verkon läpi välittämättä muista. (mplsinfo.org 2017.)

2.1 Leimakytkentä

MPLS tekniikka hyödyntää reitityksessä IP-osoitteiden sijaan leimoja. IP-paketin saapuessa MPLS-pilven reunalle lukee reunareititin kohde IP-osoitteen. Tämän jälkeen reititin laittaa IP-osoitteen päälle leiman (kuva 1), joka vastaa kohdereitittimen IP-osoitetta ja laittaa paketin menemään eteenpäin verkossa. Tästä johtuen seuraavan reitittimen ei tarvitse lukea pitkää IP-osoitetta ja verrata sitä omaan reititystauluun.



Generic MPLS Label Format

Kuva 1 MPLS-kehys (RF Wireless World 2012b)

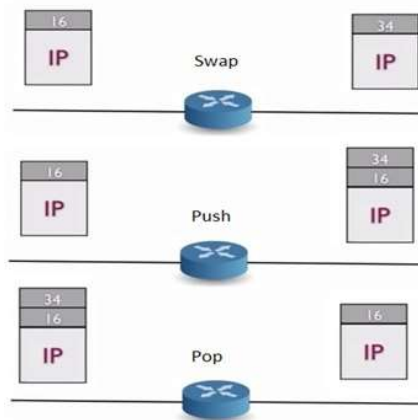
Sen sijaan se lukee leiman ja vaihtaa sen nopeasti uuteen, kohdeosoitetta vastaavaan leimaan, ja laittaa paketin eteenpäin verkossa. Verkon käyttö nopeutuu, sekä kuorma laskee, sillä suuria reititystauluja ei tarvita MPLS-pilven sisällä. Kun paketti saapuu verkon toiselle reunalle, ottaa reunareititin leiman pois osoitteen päältä ja laittaa paketin eteenpäin normaalissa IP-verkossa sen kohdeosoitteen mukaisesti. (Cisco Systems 2016.)

2.2 MPLS-operaatiot

MPLS valmiilla reitittimellä on kolme erilaista mahdollisuutta käsitellä pakettia (kuva 2), kun se saapuu reitittimeen. Näitä kutsutaan PUSH-, SWAP- ja POP-operaatioiksi. PUSH-operaatiossa MPLS-reititin lisää leimapiinon päälle uuden leiman. SWAP-operaatiossa MPLS-reititin vaihtaa leimapiinon päällimmäisen leiman toiseen leimaan. POP-operaatiossa MPLS-reititin ottaa pinon päällimmäisen leiman pois. (De Ghein 2007.)

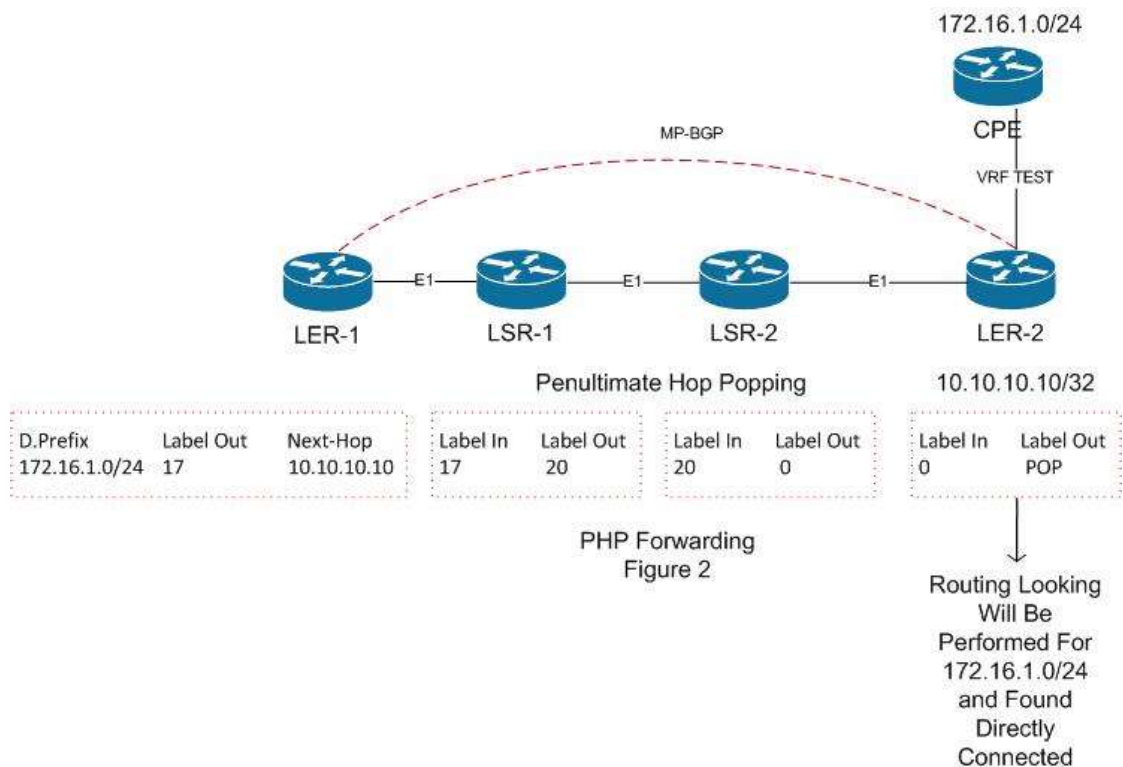
Kun paketti ensimmäistä kertaa saapuu MPLS-verkon reunalle, valitaan sille Forward Equivalence Class (FEC). Keskenään samanlainen data saa saman

FEC:in toistensa kanssa ja sen avulla määritellään paketin tarvitsema palvelu ja operaatiot. (De Ghein 2007.)



Kuva 2 MPLS-paketin operaatiot (RF Wireless World 2012a)

Penultimate Hop Poppingilla (PHP) tarkoitetaan MPLS-pilven viimeistä edellisenä olevan reitittimen toimintoa, jolla se ottaa valmiiksi päällimmäisen leiman pois paketin päältä (kuva 3). Se voi tehdä tämän, koska reitittimen next-hop-osoite kyseiselle leimalle on reunareititin. Tällä tavalla säästetään reunareitittimen laskentatehoa, sillä se ei löydä omaa leimaansa paketin päältä, vaan pelkän IP-osoitteen, tai alla olevan leiman.



Kuva 3 PHP-toiminto LSR-reitittimellä (Jain, S. 2008)

Ilman PHP:tä joutuisi reunareititin ensin suorittamaan pop-toiminnon paketille, jonka jälkeen se vasta näkisi sille tarkoitetun leiman tai IP-osoitteen.
(De Ghein 2007.)

2.3 LDP ja BGP-LDP

MPLS Label Distribution Protocol (LDP) on protokolla, joka mahdollistaa leimareitittimien leimatietojen jakamisen, pyytämisen ja irrottamisen. Sen avulla leimareititin voi ilmoittaa viereiselle reitittimelle leimat jotka se on tehnyt eri reiteille, sekä omalle loopbackille. Tämän jälkeen reitittimet neuvottelevat yhdessä Label Switched Pathin (LSP), joka mahdollistaa leimojen kulkemisen reitittimien välillä. Samoja leimoja voi olla useita MPLS verkoissa, sillä reitittimen asettama leimanumero on ainoastaan paikallisesti merkitsevä. Tällöin esimerkiksi PE-reitittimeen kohti kulkevilla reiteille voi olla monta erinumeroista leimaa, vaikka kaikilla on sama päätepiste. (Cisco Systems 2005.)

LDP voidaan myös konfiguroida targeted-LDP moodiin, jolloin LDP-tietoja vaihdetaan kahden reitittimen välillä, jotka eivät välttämättä ole naapureita. Tätä tekniikkaa käytetään erityisesti MPLS Layer2 ja Layer3 Virtual Private Network -ratkaisuisissa. Tällöin tunnelin päätäreitittimet saavat toisiinsa LDP-naapuruuden, jolloin molemmat tietävät mitä leimaa käyttää tunnelin avulla liikennöidessä. (Cisco Systems 2005.)

LDP selvittää parhaan reitin kohdeosoitteeseen Interior Gateway Protokollan (IGP) avulla, joista yleisimpiä ovat Open Shortest Path First (OSPF) ja Intermediate System-to-Intermediate System (IS-IS) protokollat. Tämän takia LDP tarvitsee aina toimiakseen IGP:n ja samalla se on myös riippuvainen sen toiminnasta. Kun LDP on IGP:n avulla määrittänyt parhaan reitin toiselle reunalle syntyy kahden reunareitittimen välille koko IGP-alueen mittainen LSP. Tätä käyttäen on mahdollista implementoida MPLS palveluita ja tunneleita verkon reunalta toiselle.
(Cisco Systems 2005.)

BGP-Label-Distribution on Border Gateway Protokollan (BGP) lisäosa, jolla voidaan jakaa leimatietoja BGP:n mukana LDP:n sijaan. Seamless MPLS-ratkaisussa tämä on tärkeää, sillä normaalin LDP:n käyttäessä IGP-protokollaa

leimatietojen vaihtamiseen katkeaa sen LSP ABR-reitittimiin, eli IGP-alueiden rajalle. BGP-Label-Distributionin BGP-next-hop-self komentojen avulla saadaan leimatiedot vaihdettua myös IGP-rajojen ulkopuolelle, sillä BGP ulottuu koko Seamless MPLS-verkon alueelle. Tällä tavoin myös skaalautuvuus paranee, sillä BGP levittäytyy suurelle verkon alueelle, mutta ei tarvitse tietoa kaikista reitittimistä matkalla. (Cisco systems 2015a.)

2.4 MPLS-TE

Multi Protocol Layer Switching Traffic Engineering (MPLS-TE) on tärkeä osa nykyaikaisia MPLS-verkkoja. Se on jatke normaalille traffic-engineering-tekniologialle (TE), johon on lisätty useita MPLS-verkkoa tukevia ominaisuuksia. Normaalissa paketin reitityksessä reititin katsoo paketin next-hopin sen hyppyjen määrän perusteella kohdeosoitteeseen ja laittaa kaikki samaan kohteeseen menevät paketit samaan suuntaan. TE-implementaatioissa paketille katsotaan paras reitti eri parametrien avulla, esimerkiksi linkkien nopeuksia vertailemalla. (Lakshman & Lobo 2006.)

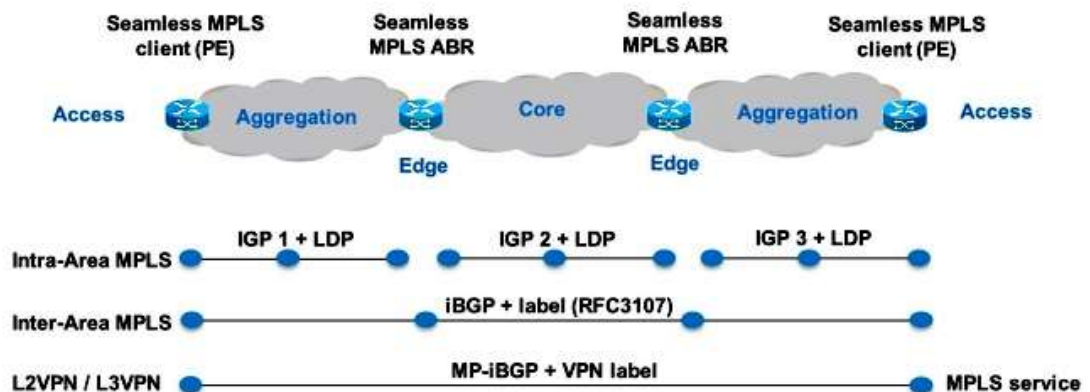
MPLS-TE:n tärkein ominaisuus on sen mahdollisuus ohjata liikennettä eri kautta, kuin normaalissa IP-reitityksessä. Tästä johtuen MPLS-TE on erinomainen teknologia kuormantasaukseen ja se onkin sen päätehtävä MPLS-verkoissa. MPLS-TE-tunnelit tehdään verkon reunasta reunalle, jolloin saadaan yhtenäinen tunneli reunareitittimien LSP:n kanssa. (Lakshman & Lobo 2006.)

Resource Reservation Protocol (RSVP) on protokolla, jonka avulla on mahdollista varata verkosta resursseja, kuten kaistanleveyttä, sekä hallita esimerkiksi quality-of-service (QoS) palveluita. MPLS-verkoissa on normaalisti käytössä sen jatke RSVP-TE. MPLS RSVP-TE:n avulla voidaan hallita koko LSP:n traffic engineeringiä kerralla, jolloin tietylle LSP:lle voidaan esimerkiksi varata tietty määrä resursseja verkosta, sekä valvoa koko tunnelia samalla kerralla. (Cisco systems 2017.)

3 SEAMLESS MPLS

Seamless MPLS:n tarkoituksena on helpottaa suurten verkkojen hallintaa ja tarjota selkeästi segmentoitu verkko, johon on mahdollista lisätä ja poistaa osia, ilman verkon palveluntarjonnan kärsimistä. Se mahdollistaa koko paketin reitin kontrolloinnin verkon päästä päähän yhdellä hallinnointitasolla ja myös vastaa modernin verkon tarpeisiin olla nopeasti konvergoituva, sekä tarjota suurempaa kaistanleveyttä hallinnointiratkaisujen pienentyessä. Sillä onkin lähes loputon skaalautuvuus ja suuret Seamless MPLS-verkot voivat helposti sisältää kymmeniä tuhansia solmuja. (Cisco Systems 2015a.)

Seamless MPLS on uusien verkkotrendien mukainen teknologia, joka siirtää verkossa tapahtuvan reitinlaskemisen reunalle ja suuritehoiset väylät keskelle. Tätä kautta saadaan laskentakuormaa jaettua verkon jokaiselle reunalle ja verkon sisäosat voivat keskittyä hyvään vikasietoon, konvergoitumiseen ja paketin nopeaan kulkuun verkon läpi. Normaalin MPLS-verkon tavoin Seamless MPLS tukee erilaisia palveluita, joita voidaan tarjota asiakkaille end-to-end tyyppisenä ratkaisuna. (Cisco Systems 2015a.)



Kuva 4 Seamless MPLS (Cisco 2016)

Seamless MPLS:n perusideoina on tarjota asiakkaalle saumaton yhteys verkon läpi nopeasti, ilman tietoa verkon todellisesta koosta tai sisällöstä. Sen täytyy olla myös helposti skaalattava ja helposti hallittava. Se rakentuu ydinalueesta, keräilyalueesta ja asiakkaan rajapinnasta, eli pääsyalueesta (kuva

4). Jokaisen alueen sisällä on oma verkko, joka ei ole IGP-yhteydessä samanlaisen alueen verkkoon. Verkot yhdistetään toisiinsa reunareitittimillä ja niiden välillä liikennöidään BGP-protokollalla, jonka avulla myös MPLS-palvelut saadaan koko suuren verkon alueelle. Yksi sen suurista vahvuuksia onkin kuljetustason ja palvelutason erottaminen. Seamless MPLS on ideana nuori, mutta siinä käytetään vanhoja tekniikoita hyväksi uudella tavalla. (Cisco Systems 2015a.)

Seamless MPLS tarvitsee jo valmiin verkon osat ja tästä syystä se onkin varsinakin suuremmissa verkoissa hyvin työläs toteuttaa. Toimiakseen oikein Seamless MPLS tarvitsee koko verkon mittaisen LSP:n ja tämän saavutettua on siinä mahdollista tarjota kaikkia samoja palveluita, kuin normaalissa MPLS-verkossa. (Cisco Systems 2015a.)

3.1 Verkon rakenne

3.1.1 Pääsyverkko, PE ja CE

Pääsyverkko on Seamless MPLS verkon uloin alue. Yleensä palveluntarjoajan MPLS-alue loppuu Provider Edge (PE) -reitittimeen, mutta erityistapauksissa se on mahdollista jatkaa PE-reitittimen läpi pääsyverkon puolelle esimerkiksi on-demand muodossa Customer Edge (CE) -reitittimeen. CE-laitteita pidetään yleisesti palveluntarjoajan laitteina, vaikka ne voivatkin sijaita asiakkaan tiloissa. Pääsyverkon laitteita ovat kaikki asiakkaiden päätelaitteet ja asiakkaiden mahdolliset omat verkot. Tämä nostaa pääsyverkkojen laitemäärän monesti moniin tuhansiin ja ne vaihtelevat matkapuhelimista ja matkapuhelintor-neista aina suuriin yritysverkkoihin. (Cisco Systems 2013.)

PE-reitittimen tehtävä on yhdistää pääsyverkko ja palveluntarjoaja toisiinsa helposti ja vaivattomasti. PE-reitittimiin voidaankin yleensä yhdistää monia erilaisia laitteita ja verkkoja, niin kauan kuin niihin voidaan laittaa oletusreitti palveluntarjoajaan päin. Tällöin PE-laite mahdollistaa reitin palveluntarjoajan verkon läpi toisille asiakkaille ilman heidän tietämystä toisistaan, tai palveluntarjoajan verkosta. (Cisco Systems 2013.)

3.1.2 Keräilyverkko

Keräilyverkko on PE-reitittimen ja ydinverkon välissä oleva alue. Sen tarkoitus on yksinkertaisesti yhdistää monia pääsyverkkoja yhteen ydinverkkoon. Samalla se mahdollistaa pääsyverkkojen PE-reitittimien keskustelun keskenään, vaikka ne olisivat eri pääsyverkoissa.

Alue voi olla satojen reitittimien kokoinen, joten se tarvitsee toimiakseen tiedon muista alueen reitittimistä. Yleisesti tähän käytetään IGP link-state reititysprotokollia, tarkemmin OSPF tai IS-IS, sillä MPLS-traffic-engineering tarvitsee toimiakseen link-state-protokollan sen käyttämien ominaisuuksien takia. Myös MPLS-LDP käyttää IGP-protokollaa leimojen levitykseen alueen sisällä ja mahdollistaa LSP:n alueen läpi. Keräilyverkkojen reititys erotetaan toisistaan IGP-alueilla ja näin ollen ne eivät voi olla yhteydessä toisiinsa ilman ydinverkkoa. (Ergun 2015.)

3.1.3 Area Border Router ja RR

Area Border Router (ABR) on ydin- ja keräilyverkkojen välissä oleva reititin, joka mahdollistaa koko Seamless MPLS-teknologian toiminnan. ABR luo käytännössä BGP yhteyden kahden eri IGP alueen välille, jolloin LSP jatkuu PE-reitittimeltä ydinverkon läpi toiselle PE reitittimelle asti.

Tämä voidaan toteuttaa kahdella eri tapaa, joista ensimmäisessä ABR voidaan asettaa mainostamaan omaa loopbackiaan ydinverkon IGP:stä eteenpäin PE-reitittimille. Toinen mahdollisuus on asettaa ABR-reitittimelle next-hop-self sen keräilyverkon puolen mainostukseen. Kummassakin tapauksessa ABR:n täytyy asettaa next-hop-self kaikkeen liikenteeseen, joka tulee ydinverkon puolelta. Jos tätä ei tehdä ei liikenne pääse kulkemaan ABR:n läpi, eikä LSP toteudu. Next-Hop-Self komento asettaa ydinverkon IGP:n puolelta tulevan liikenteen näyttämään tulevan reitittimen omasta loopbackista. Tämä mahdollistaa liikenteen kulkemisen ABR-reitittimen läpi, sillä keräilyverkoilla ei muuten olisi tietoa ABR-reitittimen takana olevista reiteistä ja se pudottaisi sinne kohdistuvat paketit. Näin ollen liikenne ohittaa IGP-reunan sen mennessä ABR-reitittimen loopbackiin, sillä ABR-reitittimellä on reitit toiselle puolelle IGP-reunaa. (Cisco systems 2013.)

Seamless MPLS-konfiguraatiossa ABR konfiguroidaan myös route-reflector-iksi. Normaali iBGP ei jaa saamiaan iBGP-reittejä toisille iBGP-naapureille ja tarvitsee siksi toimiakseen full-mesh topologian. Route-reflector hajottaa tämän iBGP-säännön ja lajittelee naapuruudet kahteen kategoriaan. Client-naapureilta saadut reitit voidaan jakaa eteenpäin rikkoen normaalin iBGP käytännön. Non-client-naapuruudet taas ovat normaaleja iBGP-naapuruuksia. Tällöin PE-reitittimet saavat tiedon muista PE-reitittimistä, sillä PE-reititin on aina client suhteessa ABR-reitittimeen, josta seuraa niiden lähetys kaikille ABR-reitittimen naapureille. (Cisco systems 2015b.)

Route-reflectorin huonona puolena on sen luoma heikko kohta verkkoon, sillä route-reflectorin kaatuessa koko verkon toiminta lakkaa. Tämä ongelma voidaan ratkaista tekemällä route-reflectorista redundanttinen ja antamalla kahdelle saman keräilyverkon route-reflector-reitittimelle sama klusteri-id. Tällöin ne muodostavat parin ja toisen kaatuessa jäljelle jäävä reitittää samalla tavalla, kuin aiemmin. (Cisco systems 2015b.)

3.1.4 Ydin

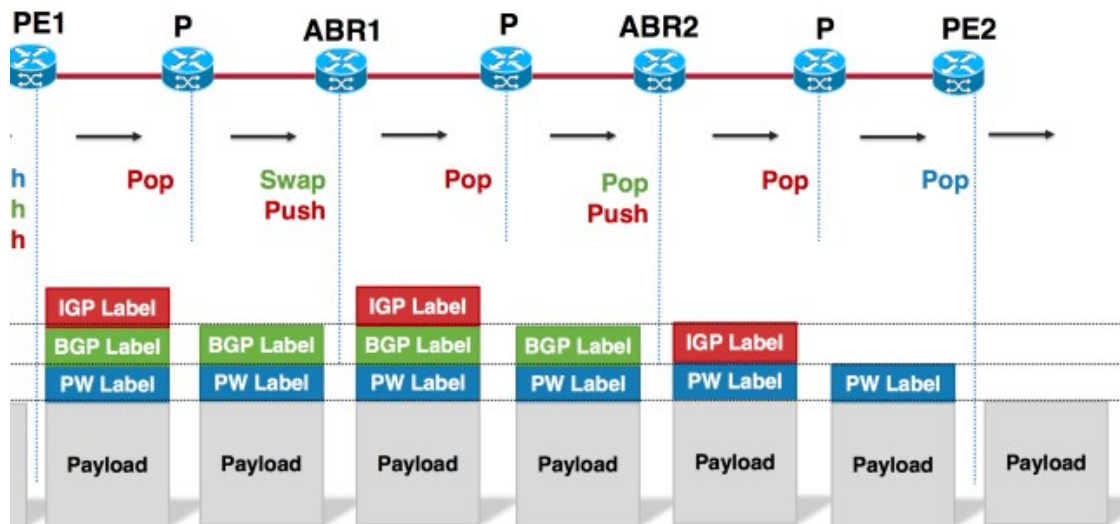
Ydinverkko on MPLS-pilven keskellä oleva verkko, joka yhdistää keräilyverkot toisiinsa, näin luoden yhteisen verkon PE-reitittimestä toiselle PE-reitittimelle. Ydinverkko voidaan toteuttaa joissain tapauksissa full-mesh topologian mukaan, sillä se yleensä sisältää huomattavasti vähemmän reitittimiä, kuin esimerkiksi keräilyverkko. Full-mesh konfiguraatio auttaa myös kuorman jakamisessa ydinverkossa. Laitteiden läpi kulkee kuitenkin huomattavasti enemmän dataa, kuin keräilyverkossa, joten ne yleensä ovat hieman tehokkaampia ja luotettavampia. (Internet Engineering Task Force 2012.)

Jotta ydinverkossa olevat laitteet voivat vaihtaa tietoja keskenään tehdään sen sisälle myös oma IGP-reititys. Ydinverkolla on myös oma IGP-alue ja näin se erotetaan keräilyverkoista, tällöin myös ABR-reitittimiin syntyy IGP-reuna ydinverkon ja keräilyverkon välille.

3.2 Leimareititys

Seamless MPLS koostuu eri alueilla toimivista MPLS-tunneleista (kuva 4, s12), joiden avulla paketti saadaan kulkemaan verkon reunalta toiselle. Alueiden tunnelit saavat leimatietonsa hieman eri tavalla ja eri protokollilla. Tästä syntyy Seamless MPLS:n työläs konfigurointi, sillä toimiakseen se tarvitsee jokaiselle alueelle useita protokollia. Näitä protokollia käytetään eri MPLS-leimatietojen levitykseen, joiden avulla saadaan Seamless MPLS-ratkaisulle tyypillinen kolmen leiman pino.

Liikennöitäessä esimerkiksi L2VPN tunnelilla Seamless MPLS-verkon läpi saa liikenne heti verkkoon sisälle tullessaan kolme leimaa. Päällimmäisenä leimana, eli IGP-leimana (kuva 5), on PE1-reitittimen laittama ABR1-reitittimen loopback leima, joka toimii BGP-next-hop osoitteena ABR1 naapuruuteen konfiguroidun next-hop-self komennon takia. PE1 oppii ABR1-reitittimen loopback leiman LDP:n avulla, sillä LDP jakaa leimat keräilyverkon IGP-osoitteiden perusteella. (Ergun 2015.)



Kuva 5 L2VPN liikenne PE1-PE2 (Ergun 2015)

Seuraavana leimapinossa on BGP-leima, joka näyttää kohti PE2-loopbackia, sillä PE1 tietää L2VPN-tunnelin toisen päään olevan PE2-reititimellä. PE1 oppii PE2 loopback-osoitteen BGP:n avulla ja saa sen tauluunsa ABR1-reitittimeltä ABR2-route-reflector iBGP reunanhajotussäännön takia. ABR1-reitittimen ja-kaessa BGP-reitin kohti PE2-loopbackia laittaa se myös BGP:n mukana leiman, joka näyttää kohti PE2-loopbackia. Tämä on mahdollista konfiguroidun

BGP-label-distributionin avulla. Leima on siis toisena, koska se on BGP-reitti kohti PE2 reititintä. (Cisco Systems 2015b; Ergun 2015.)

Alimpana leimapinossa on L2VPN leima. PE1 neuvottelee sen PE2-reitittimen kanssa targeted LDP:n avulla. Targeted LDP on mahdollista koko verkon yli, sillä BGP-yhteyden kautta ne voivat vaihtaa leimoja keskenään BGP-label-distributionin avulla. Tällöin liikenteen lähtiessä PE1 reitittimeltä on sillä IGP-BGP-L2VPN leimapino.

ABR1-reitittimelle saapuessa on leimapinosta otettu P-reitittimen penultimate-hop-popping toiminnolla pois IGP leima. Tällöin päällimmäisenä leimana ABR1-reitittimelle saapuessa on PE1:n asettama PE2-loopback leima. Tällöin ABR1-vaihtaa leiman oman PE2-loopback leiman kanssa, jonka se on asettanut BGP:n avulla saadulle PE2-loopback osoitteelle. Se laittaa BGP-leiman päälle ABR2-reitittimen loopbackia kohti olevan IGP-leiman, sillä se on PE2-BGP-reitin next-hop osoite. (Ergun 2015.)

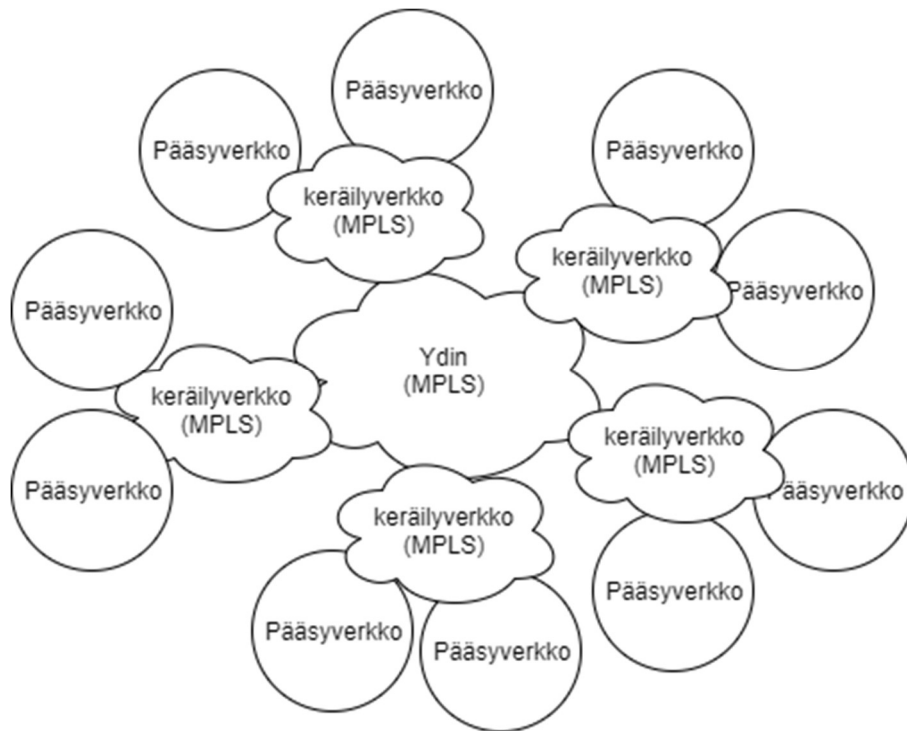
ABR2 reitittimelle tultaessa on P reitin suorittanut liikenteelle PHP-toiminnon ja ottanut päällimmäisen IGP-leiman pois. ABR2 vaihtaa ABR1:n laittaman BGP-leiman LDP-leimaan, sillä se tietää IGP:n avulla PE2-reitittimen osoitteen. Tällöin ABR2 reitittimeltä lähdettäessä kohti keräilyverkkoa on liikenteellä enää kaksi leimaa.

P-reitin suorittaa PHP-toiminnon ennen PE2-reitittimelle pääsyä, jolloin ainoa leima, joka saapuu PE2-reitittimelle asti, on PE1:n liikenteelle asettama L2VPN leima.

3.3 Hierarkia

Hierarkia on tärkeä osa Seamless MPLS-verkkoja ja sen avulla estetään turha tietojen vaihtaminen alueiden välillä. Seamless MPLS-verkot ovat tähtitopologian mallisia (kuva 6), jossa ydinalue on tähden keskellä ja siitä lähtevät haarat ovat keräilyverkkoja. Näin keräilyverkot koskevat tähden sakaroiden päässä olevia pääsyverkkoja, sekä keskellä olevaa ydinverkkoa, mutta eivät toisiaan. Pääsyverkot eivät myöskään saa koskettaa toisiaan. Hierarkian avulla voidaan erottaa alueet paremmin toisistaan, sekä lisätä alueiden sisälle

laitteita ilman muiden alueiden häiritsemistä. Tämä myös mahdollistaa keräily ja pääsyverkkojen suuruuden ja monimutkaisuuden piilottamisen. Topologiasta johtuen myös protokollien on noudatettava samaa hierarkiaa. (Internet Engineering Task Force 2012.)



Kuva 6 Tähtitopologia Seamless MPLS-verkossa

IGP protokollien täytyy myös noudattaa samaa hierarkiaa, joten OSPF-protokollaa käytettäessä on ydinalueen oltava area 0 tai vastaava. Samalla tavalla IS-IS-protokollaa käytettäessä konfiguroidaan ydinalue ISIS L2-alueeksi ja keräilyalueet ISIS L1-alueiksi. Näin IGP tietää mikä on sen topologinen runkoverkko, eikä jaa vääriä reittejä alueiden reunojen yli. (Internet Engineering Task Force 2012.)

3.4 Skaalautuvuuden parantaminen

Seamless MPLS:n perusideoihin lukeutuva skaalautuminen on tärkeä osa verkon suunnittelua. Siksi varsinkin suurissa verkoissa on tärkeää valita oikeanlaiset laitteet verkon alueille, sillä esimerkiksi PE-reitittimiä voi olla tuhansia, jolloin reititystaulut kasvavat pienemmille reitittimille mahdottoman suuriksi näiden etsiessä toisensa BGP:n avulla. Esimerkiksi normaalitilanteessa LDP-

reititin jakaa omat leimatietonsa naapurireitittimien kanssa. PE-reitittimen jaksessa omat leimansa keräilyalueen reitittimelle syntyy sille LSP koko verkkoon ja se saa BGP-reitit kaikkiin toisiin PE-reitittimiin, joita voi olla tuhansia.

3.4.1 MPLS Downstream-On-Demand

Downstream-on-demand (DoD) on tekniikka, joka on käytössä varsinkin suurimmissa Seamless MPLS ja MPLS-verkoissa. Tällöin MPLS-alue jatkuu PE-reitittimen läpi CE-laitteelle. Nämä CE-laitteet ovat yleensä kevyitä eikä niihin mahdu suuria MPLS-leimatauluja. Tällöin on-demandin avulla ne saadaan kuitenkin liittymään palveluntarjoajan suureen MPLS-verkkoon MPLS-tekniikalla, ilman suurta MPLS-leimataulua. (IETF 2013.)

Downstream-on-demand otetaan käyttöön Cisco IOS XrV-reitittimessä LDP-konfigurointi moodissa komennolla *mpls ldp downstream-on-demand with (access-list)*. Komentoon lisättävä access-list sisältää listan LDP-naapureiden ID:stä, jotka ovat myös konfiguroitu on-demand moodiin. Komento on laitettava molempiin päihin naapuruutta, jotta se toimii. Tällöin paketin saapuessa CE-reitittimeen pyytää se edeltä verkosta paketin next-hop-osoitetta vastaavan leiman. Leiman saatuaan se laittaa leiman omaan MPLS-tauluun ja jakaa paketin verkkoon next-hop-leiman mukaisesti. Se ei siis saa koko verkon leimoja, vaan pelkästään sen liikennöimiseen tarvitsemat leimat. (Cisco Systems 2014.)

3.4.2 Segment routing

Segment routing on uusi tekniikka, joka voisi tulevaisuudessa syrjäyttää LDP-protokollan IGP:n sisällä. Segment routing toimii leimojen sijaan segmentin tunnisteilla. Sen vahvuutena pidetään parempaa vikasietoa LDP:n sijasta ja helpompaa vianetsintää. Myös skaalaus on helpompaa segment routingissa, sillä paikallisten leimojen sijaan segmentin tunnisteet ovat globaalisti määräviä, jolloin tunnisteita on helpompi määrätä ja hallita. (Nokia 2016.)

4 VERKON VIKASieto

Seamless MPLS-verkkojen ollessa käytössä internetin runkoverkoissa ja suurissa yritysverkoissa, on niiden vikasiedon oltava huippuluokkaa. Redundanttisuus on tärkeää jokaisella Seamless MPLS-tasolla ja siksi se täytyykin aina ottaa huomioon verkkoa luodessa.

4.1 Palvelu- ja kuljetustason redundanttisuus

Palvelutason redundanttisuus on normaalin MPLS:n tapaan yleensä L2VPN- ja L3VPN-redundanttisuuden käyttöä ja ne käytännössä perivät redundanttisuuden kuljetustason redundanttisuudesta LSP-tunneleiden avulla. Tämä taso on helposti toteutettavissa ja hallittavissa redundanttiseksi, mutta se kärsii kaikista alemman tason vioista verkossa.

Kuljetustason redundanttisuus on huomattavasti hankalampaa sen monimutkaisuuden takia varsinkin suurissa implementaatioissa, mutta Seamless MPLS:n hierarkkinen aluejako tekee siitä mahdollista.

Kuljetustason redundanttisuus voidaan jakaa kahteen osaan, jolloin alueiden välillä ja sisällä olevissa MPLS-tunneleissa käytetään eri tekniikoita. Redundanttisuuden lisäksi on konvergoitumisen nopeus tärkeää ja siksi siihen käytetään jo valmiiksi MPLS-verkoissa käytössä olevia protokollia. Fast reroute on MPLS-verkon konvergoitumiseen käytetty yleinen protokolla ja eri laitevalmistajien laitteet voivat tukea eri versioita fast reroutesta.

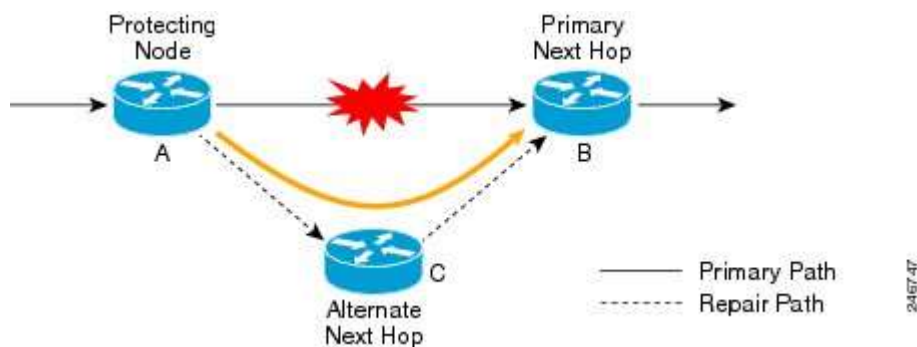
4.1.1 BGP-tunnelin redundanttisuus

Alueiden väliseen redundanttisuuteen käytetään BGP:n fast reroute ominaisuuksia. BGP fast reroute on tekniikka, jonka avulla se laskee valmiiksi varareitin BGP-yhteydelle. Kun BGP fast reroute on aktivoitu, yrittää se löytää jokaiselle BGP-yhteydelle myös varareitin. Kun se huomaa pääreitillä olevan käyttämättömissä esimerkiksi putoavan linkin kautta, vaihtaa se heti automaattisesti varareitille. Varareitin valmiudesta on hyötynä nopea vaihto, sillä varareitti on aina olemassa, sitä ei vain käytetä ennen pääreitillä vikatilaa. (Alcatel Lucent 2013.)

BGP egress node fast reroute on toinen käytössä oleva BGP:n fast reroute-jatke. Tämä on käytännössä BGP anycast, jolloin alueiden välillä olevat ABR-reitittimet saavat samanarvoisen reitin kohti PE-reititintä ja mainostavat tätä ydinverkkoon päin. Ydinverkosta tuleva paketti menee ensisijaisesti anycast master-reitittimelle, mutta sen pudotessa verkosta laitetaan paketti kohti anycast slave-reititintä. Anycastia voidaan myös käyttää ABR-reitittimien väliseen kuormantasaukseen. (Alcatel Lucent 2013.)

4.1.2 LDP-Tunneleiden redundanttisuus

Alueiden sisällä olevien tunneleiden redundanttisuus voidaan myös toteuttaa fast reroute protokollan ominaisuuksilla. Konvergoitumisen nopeus on erittäin tärkeää alueiden sisäverkoissa, joiden reititys vaikuttaa koko päällä olevaan Seamless MPLS-ratkaisuun.



Kuva 7 IP-LFA-RR (Cisco Systems 2017b)

IPv4 Loop-Free Alternate Fast Reroute (IP-LFA-FRR) (kuva 7) on Cisco Systemsin tukema teknologia, joka mahdollistaa alle 50 millisekunnin konvergoitumisen. (Cisco Systems 2015c.)

Teknologian käyttöönotossa suojaava reititin laskee ensin jokaiselle linkille varareitin. Jokaiselle linkille lasketaan myös väliaikainen korjausreitti, jonka tarkoituksen on toimia linkkinä eteenpäin verkossa verkon konvergoituessa, joka voi kestää useita satoja millisekunteja. Korjausreitti ei saa tehdä verkkoon silmukkaa takaisin samaan reitittimeen, joten se valitaan ECMP-protokollan avulla. Linkin kaatuessa vaihtaa ensin reititin paketit kohti korjausreittiä ja verkon konvergoitumisen jälkeen se jatkaa normaalisti reititystä varareitin avulla ja korjausreitti otetaan pois käytöstä, ellei se ole sama, kuin varareitti. (Cisco Systems 2015c.)

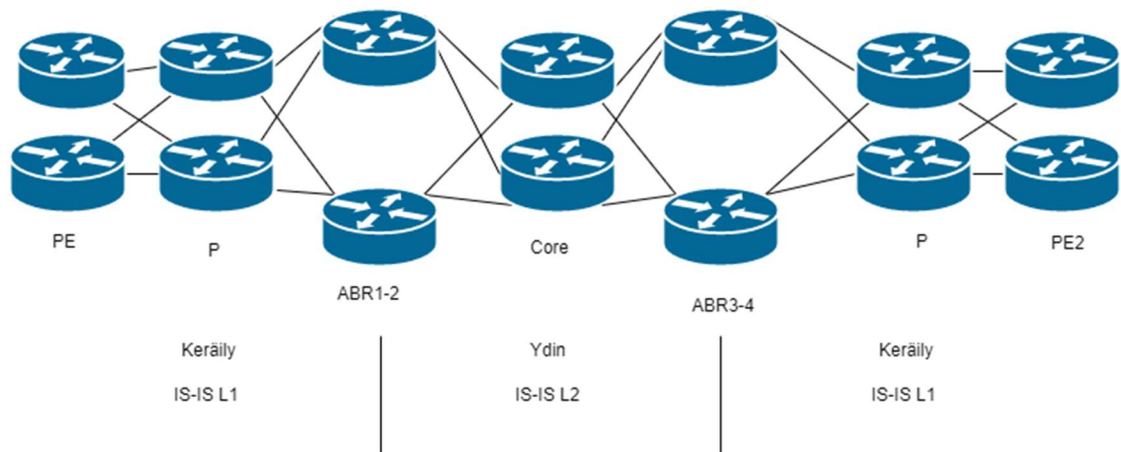
Toinen tapa alueen sisällä olevan tunnelin redundanttisuuden toteuttamiseen on valmiin vara LSP:n valitseminen MPLS-TE-FRR-protokollan avulla. Tämä mahdollistaa jopa alle 10 millisekunnin liikenteen uudelleenohjauksen. Vara IP-reittien sijaan protokolla valitsee valmiin LSP:n, jonka kautta liikenne pääsee etenemään next-hop-osoitteeseen. Tekniikkaa voidaan siis käyttää pelkän linkin ohittamiseen, mutta sillä voidaan myös ohittaa kokonainen laite. (Alcatel Lucent 2013.)

5 HARJOITUSTYÖ

5.1 Ensimmäinen harjoituskonfiguraatio

Verkon luonti aloitetaan IP-osoitteiden määrittämisellä jokaiseen liikennöivään porttiin. Jokaisella reitittimellä on myös hyvä olla loopback-osoite, sillä niitä käytetään eri reitittimien tunnistamiseen eri protokollissa. Tämän jälkeen jokaiselle alueelle konfiguroidaan oma IGP-protokolla, jotka erotetaan toisistaan aluenumeroilla. On myös hyvä varmistaa IGP-hierarkia ja varmistaa ettei IGP-reittejä ole väärillä puolilla ABR-reitittintä. Varmistamisen jälkeen vuodetaan ABR-reitittimien loopback-osoitteet keräilyyn puolelle. Seuraavaksi ABR-reitittimille luodaan BGP-naapuruudet keskenään, sekä konfiguroidaan route-reflector naapuruus PE-reitittimien kanssa. BGP:n toimivuuden toteuttamisen jälkeen voidaan antaa porteille lupa liikennöidä MPLS-protokollalla, jonka jälkeen koko verkon LSP nousee ylös.

Kahden ensimmäisen harjoituksen alustana toimi Jaakko Nurmen ohjelmoima Linux-pohjainen virtuaaliympäristö. Sen tarkoituksena oli simuloida oikeaa fyysistä ympäristöä, jossa kyseinen implementaatio olisi mahdollinen. Ympäristöön laitettiin ensimmäisessä harjoituksessa 9 virtuaalireitittintä ja toisessa harjoituksessa määrä nostettiin 14 reitittimeen (kuva 8). PE-reitittiminä ja alueiden sisäreitittiminä toimi vähemmän tehoa vaativat Cisco IoSv-reitittimet ja muihin reitittimiin asennettiin käyttöjärjestelmäksi Cisco XrV 5.3.2. Itse alusta toimi normaalissa työpöytä Windows 7:ssä.



Kuva 8 toisen harjoituksen topologia

Ensimmäisen konfiguraation tarkoitus oli tutustua lähemmin Cisco XrV:n toimintaan, tarkemmin sen MPLS-komentoihin ja yleiseen konfigurointiin.

Ensimmäiseksi konfiguroitiin kolme eri OSPF aluetta, jotka nimettiin kolmen eri Seamless MPLS-alueen nimien mukaan. Tämän jälkeen verkon molempiin reunoihin lisättiin kaksi pääsyverkossa olevaa reititintä, joiden loopback osoitteet toimittivat asiakkaiden virkaa.

Seuraavaksi oli vuorossa MPLS-konfigurointi. MPLS-konfigurointivaiheessa löydettiin eroavaisuuksia Cisco XrV-konfiguroinnissa verrattuna jo opittuihin laitteisiin, lisäksi jo tehdyn OSPF-konfiguraation naapuruudet alkoivat kaatuilla MTU-ongelmista johtuen. Lopulta tultiin siihen tulokseen, että OSPF ei toimi oikein kyseisessä XrV-versiossa alustan avulla, mutta se saatiin toimimaan MTU:ta muokkaamalla. Tätä konfiguraatiota ei saatu koskaan toimimaan oikein Seamless MPLS:n näkökulmasta, mutta se ei ollutkaan harjoituksen alkuperäinen tarkoitus.

5.2 Toinen harjoituskonfiguraatio

Toisen harjoituksen tarkoituksena oli tuottaa virtuaaliympäristössä todellinen Seamless MPLS-konfiguraatio. Opettajan ohjeesta myös OSPF vaihdettiin IS-IS-protokollaan. Huolena oli konfiguraation raskaus ja Windows-pöytäkoneen laskentateho.

Työ alkoi tutustumisella IS-IS protokollaan, sillä sitä oli käytetty huomattavasti harvemmin opetustunneilla, kuin OSPF-protokollaa. Konfigurointi alkoi IP-

osoitteiden määrittämisellä ja linkkien toimivuuden tarkistamisella. Tämän jälkeen jokaiselle Seamless MPLS-alueelle luotiin oma alue IS-IS konfiguroinnin mukaisesti.

Seuraavaksi oli vuorossa BGP-naapuruuden muodostaminen ABR-reitittimien välillä, sekä PE-reitittimien ABR-naapuruus. Näiden muodostamisessa käytettiin laitteiden loopback-osoitteita. Jotta BGP naapuruus saatiin muodostettua ABR:n ydinverkon loopbackin ja PE-reitittimen välille, vuodettiin se keräilyverkon alueen IS-IS-mainostukseen. ABR-reitittimet asetettiin myös route-reflector tilaan naapuruudessa PE-reitittimien kanssa ja niille määritettiin sama klusteri-ID viereisen ABR-reitittimen kanssa. Next-hop-self komento lisättiin jokaiseen ABR naapuruuteen, jotta route-reflectorin kautta tulevat iBGP reitit saatiin näkyviin.

```
neighbor 10.100.0.1
  remote-as 1
  cluster-id 123
  update-source Loopback0
  address-family ipv4 unicast
    next-hop-self
```

MPLS-konfigurointi alkoi sen aktivoimisella haluttuihin portteihin, sekä muokkaamalla MTU isommaksi, jotta leimatut paketit mahtuvat kulkemaan porttien läpi. LSP ei kuitenkaan tässä vaiheessa tullut valmiiksi ja alkoi vianetsintä.

Tuli selväksi, etteivät MPLS-leimat menneet perille ja ABR-reitittimiin ruvettiin tekemään muutoksia. Ensin niihin määritettiin uusi route-policy, jolla varmistettiin next-hop-self-komennon toimivuus.

```
route-policy nexthop
  set next-hop 10.100.0.2
end-policy
!
neighbor 10.100.0.5
  remote-as 1
  update-source Loopback0
  address-family ipv4 unicast
    route-policy nexthop out
    next-hop-self
!
```

Lisäksi reitittimen versiossa oli Ciscon tiedostama ongelma iBGP next-hopin kanssa, joten BGP:n alle lisättiin komento *ibgp policy out enforce-modifications*, joka mahdollisti next-hopin toiminnan. Leimat eivät vieläkaan matkanneet eteenpäin ja vian etsintää jatkettiin. Lopulta viaksi osoittautui puutteellinen BGP-konfiguraatio. BGP:n naapuruuksista puuttui komento, jolla niille annetaan lupa vaihtaa leimatietoja keskenään.

XrV ja IoS käsittelee BGP naapuruuksien konfigurointia eri tavalla, joten leimatietojen vaihdon aktivointi täytyi myös konfiguroida eri tavalla, vaikka reitittimet olivat BGP naapureita keskenään. Ciscon ohjeiden mukaan todettiin, että XrV konfiguraatio

```
router bgp 1
  address-family ipv4 unicast
  !
  neighbor 10.100.1.1
  remote-as 1
  update-source Loopback1
  address-family ipv4 labeled-unicast
  !
  !
  !
```

ja IoSv konfiguraatio

```
router bgp 1
  bgp log-neighbor-changes
  neighbor 10.100.0.1 remote-as 1
  neighbor 10.100.1.1 update-source Loopback0
  !
  address-family ipv4
  neighbor 10.100.0.1 activate
  neighbor 10.100.0.1 send-label
  exit-address-family
  !
```

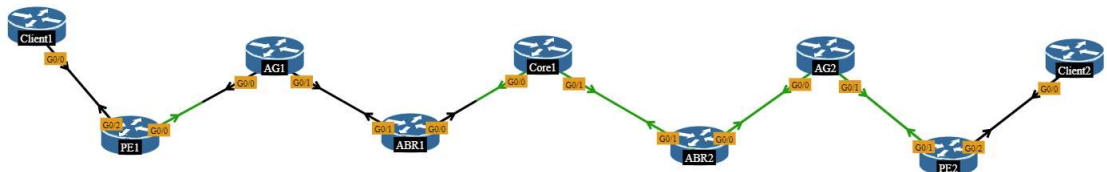
tekivät saman asian reitittimiin ja naapuruus saatiin nostettua ylös.

Tämän jälkeen LSP nousi ylös verkon päästä päähän ja L2VPN toimi koko verkon läpi Seamless MPLS-tunnelia käyttäen.

5.3 Kolmas harjoitus

Kolmannen harjoituksen tarkoituksena oli siirtää 2. harjoitus uudelle alustalle ja testata sen toimivuus uusilla laitteilla, sekä varmistaa konfiguraation oikeus.

Tarkoituksena oli myös seikkaperäisesti selvittää paketin matka verkon laidalta toiselle, jolloin esimerkiksi Seamless MPLS:n uniikki kolmen leiman pino tulee ymmärretyksi. Harjoituksen vaikeutena oli uuden alustan opettelu ja käyttäminen. Route-reflector reitittimet olivat XrV-reitittimiä ja loput reitittimet käyttivät loSv-käyttöjärjestelmää. Kolmannesta harjoituksesta jätettiin ajanpuutteen vuoksi pois redundanttisuus ja tyydyttiin yksinkertaiseen 9 reitittimen konfiguraatioon (kuva 9).



Kuva 9 Yksinkertainen Seamless MPLS-verkko

Kolmannen harjoituksen alustana toimi Jaakko Nurmen parannettu versio alkuperäisestä NestCore virtuaalialustasta. Virtualisoituja reitittimiä ajettiin Kaakkoissuomen Ammattikorkeakoulun Kotkan kampuksen tiloissa, tarkemmin ICT-laboratorion CyberLabissa. Virtuaalialustan käyttöliittymä toimi selaimen kautta ja sen avulla omaa virtuaalikonfiguraatiota pystyi muuttamaan, sekä konfiguroimaan laitteita.

Kolmanteen harjoitukseen laitettiin lisäksi PE-reitittimien taakse Client-reitittimet, joiden avulla voitiin Seamless MPLS-toiminta todentaa paremmin. Client-reitittimiin konfiguroitiin loopbackit ja yksi portti kohti MPLS-pilveä, sekä OSPF-naapuruus.

5.4 Client-Client I2VPN

Client 1 kokeilee yhteyttään client 2-reitittimeen, joten hän testaa reittiä huhuilemalla client 2-reitittimen loopbackia (kuva 10).

```
Router#ping 10.13.37.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.13.37.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms
```

Kuva 10 ping Client1-Client2

Paketin saapuessa Client 1-reitittimestä PE1-reitittimeen paketti koteloidaan L2VPN-protokollan avulla ja sille asennetaan PE1-PE2 L2VPN-tunnelia vastaava leima, jonka PE2 ja PE1 ovat neuvotelleet tunnelille. Tämä tapahtuu, koska PE1 portti G0/2 on konfiguroitu L2VPN tunneliksi PE2 portin G0/2:n kanssa.

Tämän jälkeen PE1 laittaa leimapinon päälle PE2-loopbackia vastaavan leiman, jonka se on oppinut PE2 reitittimeltä LDP-protokollalla, MPLS-BGP:n avulla. Tämän jälkeen PE1 vielä laittaa oman IGP LDP kautta oppimansa ABR1 leiman leimapinon päälle, jotta paketti voi jatkaa matkaa AG1-reitittimeen ja laittaa paketin sitä kohti. PE1-reitittimeltä lähtiessään paketilla on siis kolmen leiman pino, joka sisältää L2VPN tunnelileiman, BGP leiman, sekä IGP LDP leiman (kuva 11).

```

⊕ MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 0, TTL: 255
⊕ MultiProtocol Label Switching Header, Label: 24004, Exp: 0, S: 0, TTL: 255
⊕ MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 1, TTL: 255

```

Kuva 11 Kuvakaappaus Wireshark-ohjelmasta PE1-AG1 väliltä Client1-Client2 pingistä

Paketin saapuessa AG1-reitittimelle tutkii se leimapinoa ja näkee päällimmäisenä leiman numero 16. Omaan MPLS-forwarding tablea (kuva 12) ja PHP-sääntöä totellen se ottaa leiman pois pinon päältä ja laittaa sen ulos omasta G0/1 portista.

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	Pop Label	10.100.0.1/32	35776403	Gi0/1	10.0.1.18

Kuva 12 AG1 MPLS forwarding-table osa

ABR1 vastaanottaa paketin ja näkee päällimmäisenä leiman numero 24004. Se katsoo omasta MPLS-forwarding tablesta (kuva 13) tälle SWAP-operaation ja vaihtaa leiman numeroon 24001.

Local Label	Outgoing Label	Prefix or ID	Outgoing Interface	Next Hop	Bytes Switched
24000	Pop	10.100.1.3/32	Gi0/0/0/1	10.0.1.17	1980042
24001	17	10.100.1.1/32	Gi0/0/0/1	10.0.1.17	12037203
24002	Pop	10.100.0.3/32	Gi0/0/0/0	10.0.0.2	1976934
24003	17	10.100.0.5/32	Gi0/0/0/0	10.0.0.2	32118503
24004	24001	10.100.2.5/32		10.100.0.5	1089926047

Kuva 13 ABR1 MPLS Forwarding-table

Reititin katsoo uudelleen taulusta (kuva 13) operaation päällimmäiselle leimalle, sillä leimalla 24004 ei ole suoraan ulosvievää porttia sen ollessa BGP-naapuruus muiden reitittimien takana. Se lisää leimapinon päälle leiman numero 17, joka on BGP-next-hop osoitteen leima ja laittaa sen eteenpäin omasta Gi0/0/0/1 portista päällimmäistä leimaa totellen. Näin paketin päällä on taas kolme leimaa (kuva 14).

```

+ MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 253
+ MultiProtocol Label Switching Header, Label: 24001, Exp: 0, S: 0, TTL: 253
+ MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 1, TTL: 255

```

Kuva 14 Wireshark kaappaus ABR1-Core1

Core1-reititin saa kolmen leiman paketin ja toteaa sen olevan matkalla ulos portista G0/1. Se ottaa päällimmäisen leiman numero 17 pois (kuva 15) ja jatkaa paketin matkaa kohti ABR2-reititintä.

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	Pop Label	10.100.0.1/32	32139014	Gi0/0	10.0.0.1
17	Pop Label	10.100.0.5/32	35739851	Gi0/1	10.0.0.18

Kuva 15 Core1 MPLS-Forwarding table

ABR2-reititin suorittaa pinon päällä olevalle 24001 leimalle swap-toiminnon oman MPLS-reititystaulun (kuva 16) mukaan ja laittaa sen next-hop osoitetta

vastaavaan porttiin kohti AG2 reititintä. Tällöin siis BGP leima 24001 vaihdetaan LDP:llä opittuun leimaan 17 ja jäljelle jää vain kahden leiman pino.

Local Label	Outgoing Label	Prefix or ID	Outgoing Interface	Next Hop	Bytes Switched
24000	Pop	10.100.2.3/32	Gi0/0/0/0	10.0.2.2	1982884
24001	17	10.100.2.5/32	Gi0/0/0/0	10.0.2.2	12130162

Kuva 16 ABR2 MPLS reititystaulu

AG2-reititin suorittaa oman MPLS-reititystaulun mukaan paketille PHP-toiminnon ja jatkaa sen matkaa kohti PE2- reititintä ainoastaan L2VPN leimalla varustettuna.

Paketin saapuessa PE2 reitittimelle on päällä ainoastaan L2VPN leima, jonka se purkaa ja laittaa paketin L2VPN porttia kohti. Näin Client1-Client2 yhteyden testaus menee koko verkon läpi, mutta ne ovat tietämättömiä koko verkosta niiden välissä ja ne näkevät vain toisensa (kuva 17).

```
Router#traceroute 10.13.37.2
Type escape sequence to abort.
Tracing the route to 10.13.37.2
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.1.2 5 msec 6 msec *
```

Kuva 17 Traceroute Client 1 - Client 2 OSPF Loopback

6 PÄÄTELMÄT

Seamless MPLS on elintärkeä osa nykyisiä palveluntarjoajaverkkoja sen suureen skaalautuvuuden, sekä helpon hallinnoinnin takia. Se tuo parannuksia vanhanaikaisiin monen erillisen MPLS-alueen verkkoihin tuomalla yhteisen hallinnointitason kuinka suureen verkkoon tahansa. Se on myös runkoverkko tarpeeksi vahva kantaakseen satoja tuhansia yhteyksiä ja onkin yhä suosittu mobiililaitteiden yleistyessä huimaa vauhtia.

MPLS-palvelut kuten L2VPN ja I3VPN ovat erittäin tärkeitä palveluita yrityksille ja Seamless MPLS:n avulla nämä palvelut voidaan helposti levittää verkon reunalta toiselle ilman tietoa muista asiakkaista.

Ongelmana opinnäytetyössä oli ehdottomasti MPLS-kokemattomuus. Verkon suuruuden hahmottamisen kanssa oli myös aluksi ongelmia, sillä oikeat Seamless MPLS-verkot sisältävät tuhansia reitittimiä, jota ei voitu todentaa laboratorio-olosuhteissa. Pienenä ongelmana oli myös XrV kokemattomuus ja sen erilainen konfigurointi verrattuna tavalliseen Cisco IOS-versioon.

Mielestäni Seamless MPLS oli aiheena onnistunut, sillä se syvensi ehdottomasti tietämystä MPLS-teknologiasta, sekä aidoista operaattoriverkoista. Kiinnostavinta siinä oli ehdottomasti verkkojen suuret koot, sillä aiemmin näkemämme verkot olivat maksimissaan noin kahdenkymmenen reitittimen suuruisia.

Mielestäni opinnäytetyö käsittelee onnistuneesti Seamless MPLS-teoriaa, sekä tuo esiin sen mahdollisuudet laboratoriokäytössä. Seamless MPLS ei todennäköisesti enää hirveästi itsessään kehity, mutta esimerkiksi segment routing sen sisällä on todella kiinnostava idea. Jatkomahdollisuuksia on mielestäni monia erilaisia.

Jatkokehitysmahdollisuudet ovat mielestäni loistavat, varsinkin uuden virtuaalilustan myötä. Seamless MPLS on todella suurien verkkojen teknologia, joten kehitysmahdollisuus on ehdottomasti verkon skaalaaminen isommaksi. Verkkoon voisi esimerkiksi lisätä useita pääsy-, sekä keräilyverkkoja.

Toinen jatkomahdollisuus on Seamless MPLS:n ottaminen mukaan service-provider kurssille. Seamless MPLS on monella palveluntarjoajalla käytössä ja mielestäni se toisi ehdottomasti hyvän lisän service-provider kurssille. Sen hyötynä on myös MPLS-tietämyksen syventäminen, jota myös käydään service-provider kurssilla.

Kolmantena jatkomahdollisuutena näkisin verkon parantamisen laboratorio-olosuhteissa. Harjoitustöissä ei käyty läpi esimerkiksi traffic-engineeringiä, eikä uudella alustalla toteutettu redundanttisuutta. Tästä johtuen jatkona voisi toimia hieman suurempi verkko, jota voitaisiin viilata paremmaksi traffic-engineeringin avulla, tai miksei vaikka segment-routing implementaatiolla.

LÄHTEET

Alcatel Lucent. 2013. Evolving to “end-to-end MPLS” architectures. WWW-dokumentti. Saatavilla: https://images.tmcnet.com/online-communities/next-generation-communications/whitepapers/NP2013051418EN_Seamless_MPLS_EN_TechWhitePaper-1.pdf [viitattu 7.11. 2017]

Cisco systems, Inc. 2005. MPLS Label Distribution Protocol (LDP). WWW-dokumentti. Saatavilla: https://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t2/ftldp41.html#wp1354663 [viitattu 21.11.2017].

Cisco systems, Inc. 2013. Unified MPLS Configuration Example. WWW-dokumentti. Saatavilla: <https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/116127-configure-technology-00.html> [viitattu 7.11. 2017].

Cisco systems, Inc. 2014. Implementing MPLS Label Distribution Protocol. WWW-dokumentti. Saatavilla: https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-1/mpls/configuration/guide/b_mpls_cg41crs/b_mpls_cg41crs_chapter_01.pdf [viitattu 30.11.2017]

Cisco systems, Inc. 2015a. Unified MPLS Functionality, Features, and Configuration Example. WWW-dokumentti. Saatavilla: <https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/118846-config-mpls-00.html> [viitattu 7. 11. 2017].

Cisco Systems, Inc. 2015b. BGP Route Reflection and Multiple Cluster IDs. WWW-dokumentti. Saatavilla: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/200153-BGP-Route-Reflection-and-Multiple-Cluste.html> [viitattu 3.12.2017]

Cisco Systems, Inc. 2015c. IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3S. WWW-dokumentti. Saatavilla: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xs3s/iri-xe-3s-book/iri-ip-lfa-frr.html [viitattu 7.11. 2017]

Cisco systems, Inc. 2016. MPLS FAQ For Beginners. [online] Cisco. WWW-dokumentti. Saatavilla: <https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html#anc2> [viitattu 7. 11. 2017].

Cisco Systems, Inc. 2017a. Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide. WWW-dokumentti. Saatavilla: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_cg/mp_te_RSVP.html [viitattu 31.11.2017]

Cisco Systems, Inc. 2017b. Chapter: OSPFv2 Loop-Free Alternate Fast Re-route. WWW-dokumentti. Saatavilla:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xr-3s/iro-xe-3s-book/iro-lfa-frr.html [viitattu 21.11.2017].

De Ghein, L. 2007. MPLS Fundamentals: Forwarding Labeled Packets. *Ciscopress article* 5.1.2007. Saatavilla: <http://www.ciscopress.com/articles/article.asp?p=680824> [viitattu 7.11. 2017]

Ergun, O 2015. Seamless MPLS. Blogi. Saatavilla: <https://orhanergun.net/2015/03/seamless-mpls-architecture/> [viitattu 21.11.2017].

Internet Engineering Task Force (IETF). 2013. LDP Downstream-on-Demand in Seamless MPLS. WWW-dokumentti. Saatavilla: <https://tools.ietf.org/html/rfc7032> [viitattu 1.12.2017]

Internet Engineering Task Force, MPLS Working Group. 2012. Seamless MPLS Architecture. WWW-dokumentti. Saatavilla: <https://tools.ietf.org/html/draft-ietf-mpls-seamless-mpls-01> [viitattu 31.11.2017]

Jain, S. 2008. What is PHP (Penultimate Hop Popping). WWW-dokumentti. Saatavilla: <http://www.mplsvpn.info/2008/11/what-is-php-penultimate-hop-popping.html> [viitattu 17.12.2017]

Lakshman, U & Lobo, L. 2006. MPLS Traffic Engineering. *Ciscopress article*. Saatavilla: <http://www.ciscopress.com/articles/article.asp?p=426640&seqNum=2> [viitattu 21.11.2017].

Mplsinfo.org. 2017. Multiprotocol Label Switching (MPLS) | Network Architecture | Traffic Engineering and Migration Solutions. WWW-dokumentti. Saatavilla: <http://www.mplsinfo.org/> [viitattu 21.11.2017].

Nokia Oyj 2016. Segment Routing and Path Computation Element. WWW-dokumentti. Saatavilla: <https://resources.ext.nokia.com/asset/186949> [viitattu 31.11.2017]

RF Wireless World. 2012a. MPLS label Switching vs IP packet switching | difference between label switching and IP switching. WWW-dokumentti. Saatavilla: <http://www.rfwireless-world.com/Terminology/MPLS-label-switching-vs-IP-packet-switching.html> [viitattu 21.11.2017].

RF Wireless World. 2012b. MPLS tutorial-MPLS network,MPLS label format,MPLS providers. WWW-dokumentti. Saatavilla: <http://www.rfwireless-world.com/Tutorials/MPLS-tutorial.html> [viitattu 21.11.2017].

Statista. 2017a. Mobile internet traffic as percentage of total web traffic in August 2017, by region. WWW-dokumentti. Saatavilla: <https://www.statista.com/statistics/306528/share-of-mobile-internet-traffic-in-global-regions/> [viitattu 21.11.2017].

Statista. 2017b. Number of internet users worldwide from 2005 to 2017 (in millions). WWW-dokumentti. Saatavilla: <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/> [viitattu 21.11.2017].